



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/863,583	05/16/2001	Ikuya Morikawa	FUJA 18.671	9888

26304 7590 10/27/2005

KATTEN MUCHIN ROSENMAN LLP
575 MADISON AVENUE
NEW YORK, NY 10022-2585

EXAMINER

TRUONG, THANHNGA B

ART UNIT PAPER NUMBER

2135

DATE MAILED: 10/27/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/863,583	Applicant(s) MORIKAWA ET AL.	
	Examiner Thanhnga B. Truong	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07/25/2005 (Amendment).
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☐ Claim(s) _____ is/are allowed.
6) ☒ Claim(s) 1-28 is/are rejected.
7) ☐ Claim(s) _____ is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on 16 May 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Applicant's amendment filed on July 25, 2005 has been entered. Claims 1-28 are pending. Claims 1 and 5 are amended by the applicant.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3. Claims 1-8, 10-15, 17-19, 21-25, 27-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mashayekhi (US 5,818,936), and further in view of Ohashi et al (US 5,761,309).

a. Referring to claim 1:

i. Mashayekhi teaches:

(1) a group certificate issuing apparatus for issuing a group certificate on the client side based on original group information including the name of the group to which the related user belongs when there is said remote processing request **[i.e. referring to Figure 2, element 220 function is to generate a certificate with username/groupname and crypto key binding together (column 5, lines 34-55)]**; and

(2) a group certificate verification unit for verifying a legitimacy of said group certificate transmitted from the client side in said server, wherein said group certificate issuing apparatus adds an issuance side processed value obtained by encrypting the information of the original group information by a cryptographic function to the original group information and defines this as the group certificate **[i.e., referring to Figure 2 again, when the authentication inquiry is received at the controller, the workstation API 214 verifies that the user is a valid network client (i.e., has successively logged-on and has been authenticated to the NDS) by requesting the proper application secret for program 236. In**

response to this latter request, the database API 206 accesses the authentication database 204 and provides an encrypted application secret along with the private key for decrypting the secret. The workstation API then decrypts and forwards the proper application secret (and user identity) to the particular application program (column 6, lines 60-67 through column 7, lines 1-27). Accordingly, to effect a secure transmission of information to a recipient, a principal encodes ("encrypts") the information with the recipient's public key. Since only the intended recipient has the complementary private key, only that principal can decode ("decrypt") it. On the other hand, to prove to a recipient of information that the sender is who he purports to be, the sender encodes ("signs") the information with its private key. If the recipient can decode ("verify") the information, it knows that the sender has correctly identified itself (column 1, lines 51-60). In addition, the group of encrypted application secrets associated with the user is referred to as a "keychain." Each keychain is assigned a public/private key pair, with all secrets in the keychain being encrypted with the public key (column 3, lines 40-43)]; and

(3) said group certificate verification unit processes part of the information included in the received group certificate by an identical cryptographic function to obtain a verification side processed value and performs said authentication by confirming that said issuance side processed value and said verification side processed value coincide [i.e., Figures 4A and 4B are a flow chart of the function performed by workstation API 214 in response to the authentication request generated by a particular program. As noted, when a user 201 attempts to access a particular application program, such as a local application 240 or network-based application program 236, the particular application program requires that the user be authenticated prior to accessing its processes or data. The function begins at block 400 and proceeds to block 402 where workstation API 214 receives this authentication inquiry from the application program. Upon receipt, the workstation API 214 determines whether the user is a valid network client at block 404. If the user is not a valid network client, workstation API 214 denies the

user access to the distributed authentication service at block 406. However, if the user is a valid network client, then the workstation API 214 requests the proper application secret for the particular application program at block 410. For example, the workstation API 214 calls a "Retrieve Application Secret" API for retrieving the user's identity and proper application secrets. Workstation API 214 provides the application identifier of the particular application as part of the API call. The request to the database API 206 is preferably encoded in a network protocol element in a matter that is well-known in the art. The database API 206, in a matter described below with reference to FIG. 5, returns encrypted data and a keychain private key to the workstation API 214. At block 414, the workstation API 214 receives the encrypted data and keychain private key (column 7, lines 10-38)].

ii. Although Mashayekhi does address the authentication processes, Mashayekhi does not explicitly mention:

(1) performs said authentication by confirming that said issuance side processed value and said verification side processed value coincide.

iii. Ohashi teaches:

(1) If the encrypted Res' coincides with Res, a user certificate Cert and an authentication information AuInfo are issued for the smart card 10. Contents of the issued user certificate Cert and authentication information AuInfo are indicated in Figure 11 as an example (column 13, lines 6-10).

iv. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) have applied the coincidence of issuance and verification of a certification used in Ohashi's authentication processes into Mashayekhi's distributed network system in order to confirm that a user who requests network services or communications (hereinafter called as a network user) is a legitimate user, it is necessary at the network side to authenticate this user (column 1, lines 10-13 of Ohashi).

v. The ordinary skilled person would have been motivated to:

(1) have applied the coincidence of issuance and verification of a certification used in Ohashi's authentication processes into Mashayekhi's distributed network system for identifying a user by network when the user intends to get network services (**column 1, lines 4-6 of Ohashi**).

b. Referring to claim 2:

i. Mashayekhi further teaches:

(1) wherein said group certificate issuing apparatus includes secret information assigned to said groups in said original group information and performs the processing by said cryptographic function, said group certificate verification unit includes said secret information assigned to the groups in part of information included in said received group certificate and performs the processing by said cryptographic function, and said group certificate issuing apparatus and said server share identical secret information for identical groups [**i.e., the group of encrypted application secrets associated with the user is referred to as a "keychain." Each keychain is assigned a public/private key pair, with all secrets in the keychain being encrypted with the public key. The user may be associated with one or more keychains, each of which may be further associated with different secrets. Since these secrets correspond to application programs, the association of programs to keychains may be based upon various characteristics, such as the user's rights with respect to the programs. Furthermore, each application program may be accessible by the same or different users so that, e.g., those users having the same access rights for a program may utilize the same keychain containing each user's secrets for the programs (column 3, lines 40-53)**].

c. Referring to claim 3:

i. Mashayekhi further teaches:

(1) wherein said cryptographic function is a hash function [**i.e., a user logs into the workstation with the user's password and the workstation derives a secret, non-complimentary, encryption key by applying a known hash algorithm to the password (column 2, lines 5-8)**].

d. Referring to claims 4-6:

Art Unit: 2135

i. These claims have limitations that is similar to those of claim 1, thus they are rejected with the same rationale applied against claim 1 above.

e. Referring to claims 7-8, 18-19:

i. These claims have limitations that is similar to those of claim 3, thus they are rejected with the same rationale applied against claim 3 above.

f. Referring to claim 10:

i. Mashayekhi further teaches:

(1) wherein it cooperates with a unique ID generation means provided in said client, and the unique ID generation means generates an authentication ID for mutual authentication between said client and said server, contains the authentication ID in said group certificate, and transmits the same to said server [i.e., the flexible association of users, keychains and application secrets enables each user to have its own unique user identity and application secret for every application on the network. Thus, knowledge of one application secret does not compromise the security of all remaining application secrets associated with the user (column 4, lines 20-25). In addition, for every valid network user, the attributes of user object 302 include a login public/private key pair and a secret (e.g., the hash of the password). The user object 302 is accessed by the NDS to initially authenticate the user when the user logs on to the network. An application object 306 includes, for an associated application program, a program name, a list of users that have authority to access the program, and an application program identifier (ID). The program name attribute is a unique descriptive term that identifies the application program. The ID is a unique character string typically supplied by the application manufacturer that identifies the application program. However, the present invention reserves a pre-assigned range of IDs for programs that have no IDs assigned to them by their manufacturer. In the preferred embodiment of the present invention, the ID is an ASN.1 (abstract syntax notation; a CCITT/ISO standard) compliant identifier defined as a "Free Form Identifier." (column 6, lines 21-39)].

g. Referring to claims 11, 21:

i. These claims have limitations that is similar to those of claims 1 and 10, thus they are rejected with the same rationale applied against claims 1 and 10 above.

h. Referring to claim 12:

i. Mashayekhi further teaches:

(1) wherein it cooperates with an encryption processing unit provided in said client, and the encryption processing unit establishes an encryption session from the client to said server with said temporary password as an encryption key **[i.e., a user logs into the workstation with the user's password and the workstation derives a secret, non-complimentary, encryption key by applying a known hash algorithm to the password (column 2, lines 5-8)].**

i. Referring to claim 13:

i. Mashayekhi further teaches:

(1) wherein provision is made of a log file for recording the log of the session according to each said remote processing request for each of said users, and supervision of each user is performed based on the log **[i.e., referring to Figure 1, in general, each of the computer nodes includes memory means 108 for storing software programs and data structures associated with the cryptographic methods and techniques (column 5, lines 1-5)].**

j. Referring to claims 14, 23-24:

i. These claims have limitations that is similar to those of claim 13, thus they are rejected with the same rationale applied against claim 13 above.

k. Referring to claim 15:

i. This claim has limitations that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

l. Referring to claim 17:

i. Mashayekhi further teaches:

(1) wherein provision is made of a user-group mapping storage means, and in the user-group mapping storage means, a plurality of different groups can be assigned for one said user **[i.e., the novel distributed service 201**

comprises an exchange controller 207 coupled to an authentication database 204 containing a group of encrypted application secrets associated with the user (column 5, lines 60-64). Furthermore, the authentication database 204 is preferably a novel secure database containing groups of application secrets for predetermined application programs. Each group of application secrets, referred to as a "keychain", is assigned a public/private key pair by the KG 218 when the keychain is created. The database 204 also contains user objects which associate a given user with one or more keychains. The database API 206 manages the authentication database 204 in response to queries generated by workstation API 214. (column 6, lines 3-11)).

m. Referring to claim 22:

i. This claim has limitations that is similar to those of claim 12, thus it is rejected with the same rationale applied against claim 12 above.

o. Referring to claim 25:

i. This claim has limitations that is similar to those of claim 10, thus it is rejected with the same rationale applied against claim 10 above.

p. Referring to claim 27:

i. Mashayekhi further teaches:

(1) wherein it cooperates with a group certificate temporary storing unit provided in said server, and, when the assignment of a plurality of different groups is enabled for one said user, it verifies said group certificates received from said client, stores them in the group certificate temporary storing unit, and switches and uses the stored group certificates in accordance with said predetermined authorization necessary for the request with respect to the following remote processing requests [i.e., Figure 2 discloses a certificate storage server (CSS) node for storing certificate (column 4, lines 47-48). Furthermore, the workstation and server nodes may be configured as a distributed authentication service 201 that automates an authentication exchange between a user interface 112 200. The novel distributed service 201 comprises an exchange controller 207 coupled to an authentication database 204 containing a group of encrypted application secrets

associated with the user. The controller 207, in turn, comprises an application program interface (API) that is distributed among user workstations (i.e., workstation API 214) and the authentication database (i.e., the database API 206). Illustratively, both the database API and authentication database reside in a network directory services (NDS) system (column 5, lines 57-67 through column 6, lines 1-2)].

q. Referring to claim 28:

i. This claim has limitations that is similar to those of claim 27, thus it is rejected with the same rationale applied against claim 27 above.

3. Claims 9, 16, 20, 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Mashayekhi (US 5,818,936), further in view of Ohashi et al (US 5,761,309), and further in view of Perlman (US 5,892,828).

a. Referring to claim 9:

i. Mashayekhi briefly teaches the hash algorithm, however the detail of the hash algorithm has not been shown precisely. On the other hand, Perlman teaches:

(1) Perlman's invention generally relates to a technique for verifying the presence of a user to applications stored on a distributed network system using a single password. Briefly, the technique generally comprises computing a one-way hash value of the password that is initially provided by the user to a workstation during a login procedure (**column 3, lines 34-39**). Referring to Figure 4 for the sequence of steps for dynamically verifying the presence of a user when authenticating the user to various services and applications in a distributed network system.

ii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) clearly show the sequence of steps in hash algorithm for authentication processes as in Perlman for verifying the identity of a user of a distributed network system prior to allowing the user access to system resources and applications is referred to as authentication (**column 1, lines 20-22 of Perlman**).

iii. The ordinary skilled person would have been motivated to:

(1) clearly show the sequence of steps in hash algorithm for authentication processes as in Perlman since cryptography is often used to preserve the confidentiality of the transmitted password when authenticating the user to remote applications. Furthermore, a well-known cryptographic technique used to perform remote authentication is public key cryptography, wherein a public key system may be used in such a way as to ensure that information being transmitted cannot be understood by an eavesdropper, as well as to ensure the authenticity of the sender of the information (**column 1, lines 40-54 of Perlman**).

b. Referring to claim 16:

i. This claim has limitations that is similar to those of claims 9 and 10, thus it is rejected with the same rationale applied against claims 9 and 10 above.

c. Referring to claim 20:

i. This claim has limitations that is similar to those of claims 1 and 9, thus it is rejected with the same rationale applied against claims 1 and 9 above.

d. Referring to claim 26:

i. This claim has limitations that is similar to those of claims 9 and 10, thus it is rejected with the same rationale applied against claims 9 and 10 above.

Response to Argument

4. Applicant's arguments filed July 25, 2005 have been fully considered but they are not persuasive.

Applicant argues that:

The "encrypted application secret" described in Mashayekhi is not obtained by encrypting the private key. As such, the cited portions of Mashayekhi further fails to disclose or suggest, "said group certificate issuing apparatus adds an issuance side processed value obtained by encrypting the information of the original group information by a cryptographic function to the original group information and defines this as the group certificate."

Examiner acknowledges that applicant has amended claims 1 and 5 to overcome the prior arts. However, the prior arts are still read on to the newly amended claims and examiner still maintains that:

Mashayekhi and Ohashi do teach the claimed subject matter as previously mentioned in last office action and repeats herein in this office action. Furthermore, Mashayekhi does disclose to effect a secure transmission of information to a recipient, a principal encodes ("encrypts") the information with the recipient's public key. Since only the intended recipient has the complementary private key, only that principal can decode ("decrypt") it. On the other hand, to prove to a recipient of information that the sender is who he purports to be, the sender encodes ("signs") the information with its private key (*emphasis added*). If the recipient can decode ("verify") the information, it knows that the sender has correctly identified itself (column 1, lines 51-60).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988) and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, the combination of teaching between Mashayekhi and Ohashi is sufficient.

Besides, Mashayekhi and Ohashi do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

For the above reasons, it is believed that the rejections should be sustained.

Conclusion

5. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action for claims 1-3, 5, and 7-28. Claims 4 and 6 are still maintain by the examiner. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

a. DeTreville (US 6,609,199) discloses a secure communication channel between an open system and a portable IC device is established. An application running on the open system desiring access to the information on the portable IC device authenticates itself to the portable IC device, proving that it is trustworthy (see abstract) In addition, DeTreville's system in combining with Ohashi is still read on to claims 1 and 5 of application invention (referring to Figure 3 of DeTreville).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 703-872-9306.

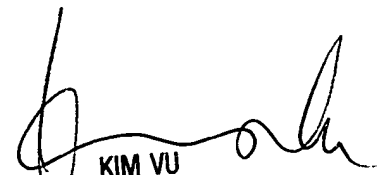
Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

Application/Control Number: 09/863,583
Art Unit: 2135

Page 13

TBT

October 18, 2005



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2135